

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

1999年 9月 6日

出 願 番 号  
Application Number:

平成11年特許願第251660号

出 願 人  
Applicant(s):

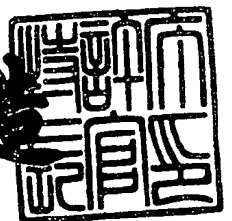
セイコーエプソン株式会社

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 8月25日

特許庁長官  
Commissioner,  
Patent Office

及川耕造



出証番号 出証特2000-3068859



【書類名】 特許願

【整理番号】 SE990305

【提出日】 平成11年 9月 6日

【あて先】 特許庁長官 殿

【国際特許分類】 H04N 5/225

【発明の名称】 デジタルカメラおよび画像改竄検出システム

【請求項の数】 6

【発明者】

    【住所又は居所】 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

    【氏名】 中島 靖雅

【発明者】

    【住所又は居所】 長野県諏訪市大和三丁目3番5号 セイコーエプソン株式会社内

    【氏名】 最上 和人

【特許出願人】

    【識別番号】 000002369

    【氏名又は名称】 セイコーエプソン株式会社

【代理人】

    【識別番号】 100093779

    【弁理士】

    【氏名又は名称】 服部 雅紀

【手数料の表示】

    【予納台帳番号】 007744

    【納付金額】 21,000円

【提出物件の目録】

    【物件名】 明細書 1

    【物件名】 図面 1

    【物件名】 要約書 1

特平 1 1 - 2 5 1 6 6 0

【包括委任状番号】 9901019

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタルカメラおよび画像改竄検出システム

【特許請求の範囲】

【請求項 1】 撮影対象からの光を画像データに変換する撮像部と、  
前記画像データから第 1 の特徴データを生成する手段と、  
公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と

前記特徴データを前記秘密鍵により暗号化する手段と、  
前記画像データに暗号化した特徴データを埋め込む手段と、  
前記第 1 の特徴データを埋め込んだ画像データを記録する記録媒体と、  
前記秘密鍵を外部記録媒体から転送する手段と、  
を備えることを特徴とするデジタルカメラ。

【請求項 2】 撮影対象からの光を画像データに変換する撮像部と、  
前記画像データから第 1 の特徴データを生成する手段と、  
公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と

前記特徴データを前記秘密鍵により暗号化する手段と、  
前記画像データに暗号化した特徴データを埋め込む手段と、  
前記第 1 の特徴データを埋め込んだ画像データを記録する記録媒体とを備え、  
前記秘密鍵は、前記秘密鍵記録部に隠し属性で記録されることを特徴とするデ  
ジタルカメラ。

【請求項 3】 撮影対象からの光を画像データに変換するデジタルカメラに  
機能を付加する方法であって、

公開鍵によって復号可能に暗号化するための秘密鍵のデータ量を、複数の大き  
さから選択する手順と、

前記秘密鍵を外部記録媒体から前記デジタルカメラの秘密鍵記録部に記録する  
手順と、

前記秘密鍵を用いてデータを暗号化するプログラムを前記デジタルカメラに導  
入する手順と、

を含むことを特徴とするデジタルカメラの機能付加方法。

【請求項 4】 前記秘密鍵は、隠し属性で記録されていることを特徴とする請求項 3 記載のデジタルカメラの機能付加方法。

【請求項 5】 請求項 1 または 2 のいずれかに記載のデジタルカメラを用いた画像改竄検出システムであって、

前記画像データを入力する手段と、

前記画像データから暗号化された第 1 の特徴データを取り除く手段と、

前記暗号化された第 1 の特徴データを復号化する手段と、

前記暗号化された第 1 の特徴データを取り除いた画像データから第 2 の特徴データを生成する手段と、

前記復号化された第 1 の特徴データと前記第 2 の特徴データとを比較する手段と、

を備えることを特徴とする画像改竄検出システム。

【請求項 6】 複数の前記秘密鍵に対応する複数の公開鍵を記録する手段を備えることを特徴とする請求項 5 記載の画像改竄検出システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、撮影した画像をデジタルデータとして記録するデジタルカメラ、デジタルカメラに機能を付加する方法、およびデジタルカメラにより記録された画像データの改竄を検出するシステムに関するものである。

【 0 0 0 2 】

【従来の技術】

従来より、写真を撮影するときには、レンズから取り込まれた光がフィルムの上に照射され、化学反応が起きることで画像が記録されるカメラが用いられている。上記のカメラでは、フィルムを現像し、印画紙に焼き付けることにより写真をプリントすることができる。上記の化学反応として一般に塩化銀の反応が利用されるため、このようなカメラによって撮影された写真を銀塩写真という。

【 0 0 0 3 】

一方、近年ではCCD等の光センサにより光を電気信号に変換し、それをデジタル信号に変換してから、フラッシュメモリ等の記録媒体に記録するデジタルカメラが普及している。デジタルカメラを用いると、パーソナルコンピュータ等の処理装置を用いて画像の保存や様々な加工を個人で手軽に行えるほか、プリンタで出力することによりフィルムの現像をすることなしに写真を印刷することができる。プリンタの印刷品質の向上により、銀塩写真とほとんど区別がつかないほど品質の高い写真も印刷できるようになってきている。

【0004】

【発明が解決しようとする課題】

しかしながら、損害保険等の証明写真に用いようとする場合など、重要な証拠写真にデジタルカメラで撮影した写真を用いると、デジタルカメラで撮影された画像はパーソナルコンピュータ等により容易に加工が可能であり、銀塩写真と比較して加工の跡を残さずに加工することが容易であるため、不正に改竄された写真が用いられていても判別することが困難であり、悪用される恐れがあるという問題がある。

【0005】

したがって、本発明の目的は撮影時の画像データから改竄されたか否かを検出することのできる画像データを出力するデジタルカメラおよびそれを用いた画像改竄検出システムを提供することにある。

【0006】

【課題を解決するための手段】

本発明の請求項1記載のデジタルカメラによれば、画像データから第1の特徴データを生成する手段と、公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と、特徴データを秘密鍵により暗号化する手段と、画像データに暗号化した特徴データを埋め込む手段と、第1の特徴データを埋め込んだ画像データを記録する記録媒体と、秘密鍵を外部記録媒体から転送する手段とを備える。したがって、デジタルカメラによる撮影時に記録媒体に記録された画像データが、その後に1ビットでも変更された場合には、画像データと第1の特徴データとが不整合となる、あるいは特徴データが破壊されるため、撮影後に画像

データが改竄されたと判断することができる。また、万一秘密鍵が他人に知られてしまったような場合であっても、別の秘密鍵を外部記録媒体から転送して書き換えることにより安全に使用することができる。

## 【 0 0 0 7 】

本発明の請求項 2 記載のデジタルカメラによれば、画像データから第 1 の特徴データを生成する手段と、公開鍵によって復号可能に暗号化するための秘密鍵を記録する秘密鍵記録部と、特徴データを秘密鍵により暗号化する手段と、画像データに暗号化した特徴データを埋め込む手段と、第 1 の特徴データを埋め込んだ画像データを記録する記録媒体とを備え、秘密鍵は秘密鍵記録部に隠し属性で記録される。そのため、秘密鍵の内容が容易に読み出されないことがない。

## 【 0 0 0 8 】

本発明の請求項 3 記載のデジタルカメラに機能を付加する方法によれば、公開鍵によって復号可能に暗号化するための秘密鍵のデータ量を、複数の大きさから選択する手順と、秘密鍵を前記デジタルカメラの秘密鍵記録部に記録する手順と、秘密鍵を用いてデータを暗号化する手段を付加する手順とを含む。これにより、簡易な暗号化でよい場合と、特に信頼性が必要な場合とで暗号化のレベルを使い分けることができる。

## 【 0 0 0 9 】

本発明の請求項 5 に記載の画像改竄検出システムによれば、画像データを入力する手段と、画像データから暗号化された第 1 の特徴データを取り除く手段と、暗号化された第 1 の特徴データを復号化する手段と、暗号化された第 1 の特徴データを取り除いた画像データから第 2 の特徴データを生成する手段と、復号化された第 1 の特徴データと第 2 の特徴データとを比較する手段とを備える。そのため、第 1 の特徴データと第 2 の特徴データとが一致していれば、入力された画像データがデジタルカメラによって記録された後に変更されていないことを検出することができる。

## 【 0 0 1 0 】

本発明の請求項 6 記載の画像改竄検出システムによれば、複数の秘密鍵に対応する複数の公開鍵を記録する手段を備える。そのため、特徴データの生成方法、

暗号化方法、画像データへの埋め込み方などのアルゴリズムを知る者が、自分で公開鍵と秘密鍵の組み合わせを作成し、本発明と同様の処理を行った場合でも、あらかじめ用意された公開鍵と異なるものであれば、その画像データは改竄された可能性があるとは判断することができる。なお、画像改竄検出システムに記録される複数の公開鍵が知られたとしても、公開鍵から秘密鍵を算出することはほぼ不可能であるため、秘密鍵が他人に知られる恐れはない。

## 【0011】

## 【発明の実施の形態】

以下、本発明の実施の形態を図面に基づいて詳細に説明する。

図2は本発明の実施例のデジタルカメラ1を説明するためのブロック図である。制御部11、集光レンズ12、光センサとしてのCCD (Charge Coupled Device) 13、A/D変換部14、RAM (Random Access Memory) 15、画像データを記録する画像記録媒体としてのフラッシュメモリ16、フラッシュメモリ16の内容を外部のパーソナルコンピュータ20と入出力するためのインターフェイス17、画像を表示可能な液晶表示部 (LCD) 19などから構成される。制御部11はCPUと、デジタルカメラ1の様々な制御を行うためのプログラムが記録されたROMと、入出力手段とを備える。フラッシュメモリ16はデジタルカメラ1に内蔵されるほか、デジタルカメラ1に着脱自在なメモリカードであってもよく、その両方を備えていてもよい。

## 【0012】

使用者は、デジタルカメラ1に設けられる入力キーへの入力により、デジタルカメラにより撮影を行う撮影モード、すでに撮影した画像を表示する再生モード、デジタルカメラの作動について種々の設定を行う設定モードなどを切り替えることができる。

## 【0013】

本実施例のデジタルカメラ1は、外部記録媒体21 (例えば、磁気ディスクやCD-ROM) に記録されたプログラムを、パーソナルコンピュータ20のような外部の処理装置からデジタルカメラ1にインターフェイス17を介して送信し、プログラムをデジタルカメラ1のフラッシュメモリ16に導入 (インストール



）することができる。プログラムを導入するためのプログラムもまた、外部記録媒体 21 に記録され、パーソナルコンピュータ 20 によって実行されることにより、プログラムのインストールが行われる。

【0014】

フラッシュメモリ 16 および外部記録媒体 21 は、格納されるデータやプログラムをファイルとして格納し、ファイルの格納位置や属性を登録するファイルアロケーションテーブルによって各ファイルを管理するように構成されている。ファイルアロケーションテーブルに登録されるファイルの属性は、実行されるプログラムに対して各ファイルを識別させるためのものであって、その属性には、いずれのプログラムからも識別可能となる通常属性と、設定したプログラムのみが識別可能となる隠し属性とがある。

【0015】

デジタルカメラ 1 にインストールされたプログラムは、デジタルカメラ 1 の制御部 11 により実行することが可能である。デジタルカメラ 1 に着脱自在なメモリカード内にプログラムを記録し、デジタルカメラ 1 に内蔵されたフラッシュメモリ 16 にプログラムを送信することにより、インストールしてもよい。プログラムのインストールは、デジタルカメラ 1 を購入後に所有者が自分で行ってもよく、また、プログラムがインストールされた状態で販売してもよい。

【0016】

本実施例では、画像データに画像の改竄を検出するためのデータとして、画像データから生成した特徴データを電子透かしの方式で画像データに埋め込む手順を含むプログラム（以下透かしプログラム）をデジタルカメラにインストールする。透かしプログラムがインストールされると、デジタルカメラ 1 で撮影が行われた時には、通常の画像記録を行うプログラムに代わって、上記の透かしプログラムが実行され、画像データがフラッシュメモリ 16 に記録される。撮影したときに通常の記録を行うか、透かしプログラムを実行させるかを、設定モードで選択できるようにしてもよい。

【0017】

透かしプログラムと同時に、画像改竄検出データを暗号化するのに必要な秘密

鍵データが外部記録媒体 21 からデジタルカメラ 1 に内蔵されたフラッシュメモリ 16 に転送される。透かしプログラムをインストールするためのプログラムを複数用意し、例えば 128 ビットの秘密鍵データがインストールされるプログラム、256 ビットの秘密鍵データがインストールされるプログラム、512 ビットの秘密鍵データがインストールされるプログラムの 3 種類の中から実行するプログラムを使用者が選択することができる。これにより、簡易な暗号化でよい場合と、特に信頼性が必要な場合とで暗号化のレベルを使い分けることができる。

【0018】

秘密鍵データは、外部記録媒体 21 およびデジタルカメラ 1 に内蔵されたフラッシュメモリ 16 の中で隠し属性のファイルとして扱われる。そのため、秘密鍵データの内容が容易に読み出されることがない。また、外部記録媒体 21 に秘密鍵データを暗号化して記録し、デジタルカメラ 1 にその暗号を復号する手段を設け、暗号が復号された秘密鍵データをフラッシュメモリ 16 に書き込むことにより、秘密鍵データをより安全に扱うことが可能である。

【0019】

また、デジタルカメラ 1 に、すでに透かしプログラムがインストールされている場合には、秘密鍵データのみを外部記録媒体 21 からデジタルカメラ 1 に導入してもよい。これにより、秘密鍵データの内容が他人に知られてしまったことが明らかになった場合などに、別の秘密鍵を転送して書き換えることにより安全に使用することができる。

【0020】

図 1 は、透かしプログラムをインストールしたデジタルカメラ 1 により撮影が行われる行程を示すフローチャートである。ユーザーがデジタルカメラ 1 のシャッターを押すと、ステップ S101 で、集光レンズ 12 により集光された光が CCD 13 に入力され、電気信号に変換される。集光レンズ 12 の絞りやシャッタースピード、すなわち CCD 13 の蓄積時間は制御部 11 によって自動的に、またはユーザーの指示によって制御される。CCD 13 として、例えば R (Red)、G (Green)、B (Blue) の原色フィルタを有する複数の画素がマトリックス状に配置された CCD 13 を用いることにより、カラー画像を撮影することがで

きる。C (Cyan)、M (Magenta)、Y (Yellow)、G (Green) の補色フィルタを有するCCDを用いる場合もある。

#### 【0021】

ステップS102では、CCD13から出力された電気信号がA/D変換部14によりデジタル信号に変換され、ステップS103ではA/D変換部14から出力されたデジタルデータが高速化のためDMA (Direct Memory Access) により制御部11を介さずに直接RAM15のアドレスを指定して記録される。RAM15としてはセルフリフレッシュ機能をもつDRAMを用いることができる。

#### 【0022】

ステップS104では、RAM15に記録されたデータについて、ホワイトバランスの調整、補間処理、色補正などの各種の画像補正が行われる。ここで、画像の拡大・縮小など、その他の画像処理を行ってもよい。

#### 【0023】

ステップS105～S110では、画像記録媒体への記録枚数を多くするためにステップS104で補正されたデータをJPEG (Joint Photographic Experts Group) などの方式により圧縮し、容量の小さな画像データを生成する。JPEG圧縮は、制御部11によってソフトウェア的に行うほか、高速化のために専用の回路を用いることができる。

#### 【0024】

以下にJPEG圧縮の手順を説明する。ステップS105では、まず画像データを $8 \times 8$ 画素を1単位とした複数のブロックに分割する。例えば、 $640 \times 480$ 画素の画像データであれば、 $80 \times 60 = 4800$ ブロックに分割され、ブロック単位に処理が行われる。

#### 【0025】

次に、B1～B480の各ブロックごとに画素同士の濃度の相対関係（空間周波数）を調べ、DCT（拡散コサイン変換）方式により、各ブロックを低周波数項のDCT0から高周波数項のDCT63に分ける。DCT0～DCT63はそれぞれ8ビットの値である。図3には、高周波数項のDCT63を16進数で示している。そして、所定の量子化テーブルを用いて量子化することにより高周波

数項の多くが0となるようにし、後の行程でハフマン符号化したときに圧縮率が高くなるようにする。

#### 【0026】

ステップS106では、後の行程で特徴データを埋め込む位置を決定するために、ブロック化されDCT変換された画像データの先頭のブロックから順に各ブロックで最も高周波側の成分であるDCT63を調べる。そして、DCT63の値が、0および1以外のブロックを埋め込みブロックとして記憶する。図3に示す例では、B3、B4、B5及びB6が①、②、③および④の埋め込みブロックとして選択され記憶される。本実施例では128ビットのハッシュ値を用いるために、128のブロックを選択する。埋め込みブロックが128ブロックに満たない場合は、足りない埋め込みブロック数と未調査のブロックが一致した時点で、残りのブロックを全て埋め込みブロックとする。そして埋め込みブロックのDCT63の最下位ビットを全て0に置き換える。これにより、例えばブロックB4のDCT63はFFからFEに書き換えられるが、高い周波数における小さな変動は、肉眼ではほとんど判断することができないため、画像の歪みは最小限となる。

#### 【0027】

ステップS107では、ステップS106で部分的に書き換えられた画像データに基づいて、制御部11により特徴データを生成する。特徴データとしては、例えば種々の一方向ハッシュ関数により算出されるハッシュ値を用いることができる。また、ハッシュ値の他に、チェックサム、CRC方式等、データがオリジナルから変更されているか否かを検出することができる公知の方法を本発明に適用することもできる。これらの方法を用いることにより、各々の画像データに対して異なる特徴データを割り当てることができ、また、特徴データから元の画像データを再現することはほとんど不可能となる。本実施例では、特徴データとして128ビットのハッシュ値を算出する。例えば、MD5、SHAあるいはRIPEMDハッシュ関数を用いることができる。

#### 【0028】

ステップS108では、ハッシュ値などの特徴データが解析されたり容易に書

き換えられたりしないように、制御部 11 により暗号化して暗号化データとする。暗号化の方法としては、公開鍵と秘密鍵を用いる RAS 方式など、公知の方法を用いることができる。秘密鍵で暗号化した暗号化データは、秘密鍵と対になった公開鍵を用いて復号化することができる。秘密鍵はデジタルカメラ 1 内に隠し属性のファイルとして記録されている。秘密鍵は、他人に知られてはならず、また、本実施例ではユーザーが秘密鍵を知る必要はない。一般に、公開鍵から、それに対応する秘密鍵を求めることは非常に困難である。これにより、画像データが同一の特徴データを得られる別の画像データに変更されることや、画像データの変更に合わせて特徴データが書き換えられるのを防ぐことができる。

## 【0029】

ステップ S109 では、ハッシュ値を暗号化した暗号化データを、選択された埋め込みブロックの DCT 63 の最下位ビットに 1 ビットずつ書き込むことにより、画像の劣化を最小限にして特徴データを画像データの中に埋め込む。なお、JPEG 形式の画像データは、カラー画像の場合は、Y（輝度）、U、V（色相）の成分を有するが、暗号化された特徴データは Y 成分に埋め込まれる。

## 【0030】

ステップ S110 では、暗号化データが埋め込まれたデータをハフマン符号化することにより、データの圧縮を行う。ハフマン符号化では、データの可逆性は満足されており、処理の前後でデータの欠損はない。S105 での量子化テーブルによる量子化の度合いを変えることによって圧縮率を変更することができる。

## 【0031】

ステップ S111 では、S110 で圧縮された画像データを JPEG ファイル 30 として画像記録媒体としてのフラッシュメモリ 16 に記録する。フラッシュメモリ 16 は通電しなくても記録内容を保存することのできる書換え可能な記録媒体であり、デジタルカメラ 1 に内蔵されるか、あるいは着脱自在にデジタルカメラ 1 に取り付けられている。一般に JPEG ファイル 30 は図 4 に示すようにデータ長、圧縮率等の情報を含むヘッダ部 31 と、画像データ部 32 とから構成される。デジタルカメラ 1 によって記録される JPEG ファイル 30 の場合は、撮影日や撮影条件等の情報もヘッダ部 31 に記録されることがある。本実施例で

は、暗号化に用いた秘密鍵に対応する公開鍵 3 3 をヘッダ部 3 1 に更に加えて記録している。

【 0 0 3 2 】

設定モードで透かしプログラムを実行しないように設定されている場合は、通常の J P E G 圧縮と同様の手順により、ステップ S 1 0 5 で D C T 変換され量子化されたデータはステップ S 1 1 0 でハフマン符号化により圧縮される。

【 0 0 3 3 】

上記の例では、J P E G 圧縮の途中の行程で特徴データを埋め込んだが、特徴データの埋め込みを行わずにハフマン符号化まで行う通常の J P E G 圧縮を行った後に、部分的に画像データを復号し、ステップ S 1 0 6 ~ S 1 0 9 と同様の行程により特徴データを埋め込み、再度ハフマン符号化してもよい。

【 0 0 3 4 】

上記のようなデジタルカメラ 1 と、デジタルカメラ 1 から出力された画像データを入力する手段を備えるパーソナルコンピュータ 2 0 等のコンピュータと、デジタルカメラ 1 によって記録された画像データが変更されたか否かを判定するためにパーソナルコンピュータ 2 0 等にインストールされた検出プログラムとによって画像改竄検出システムが構成される。

【 0 0 3 5 】

本実施例の画像改竄検出システムにより画像の改竄を検出する行程を図 5 に示すフローチャートを用いて説明する。

ステップ S 2 0 1 では、検出プログラムにより、パーソナルコンピュータ 2 0 にデジタルカメラから画像データが読み込まれる。パーソナルコンピュータ 2 0 に画像データを読み込む手段としては、シリアルケーブル 1 8 等を介してデジタルカメラ 1 のインターフェイス 1 7 と接続してフラッシュメモリ 1 6 内の J P E G ファイルをパーソナルコンピュータ 2 0 に転送する方法や、フラッシュメモリ 1 6 が着脱自在でパーソナルコンピュータ 2 0 と互換性のある形式でフォーマットされている場合には、アダプタを介してフラッシュメモリ 1 6 に記録された J P E G ファイル 3 0 をパーソナルコンピュータ 2 0 で直接読取することも可能である。

【0036】

ステップS202では、画像データを復号化し、上記のステップS106で特徴データを埋め込むブロックを選択したときと同様の手順で、特徴データが埋め込まれているべきブロックを選択し、128ビットの暗号化データを抽出する。

【0037】

ステップS203では、暗号化データが埋め込まれていたビットに全て0を書き込み、暗号化データが埋め込まれる前の元画像データを生成する。

ステップS204では、ステップS107と同様の手順で、128ビットのハッシュ値を算出する。

【0038】

ステップS205では、ステップS202で抽出した暗号化データを、JPEGファイルのヘッダに書き込まれた公開鍵を用いて、秘密鍵によって暗号化されたことを確認すると同時に暗号を復号化する。それにより、暗号化前のハッシュ値を求める。

【0039】

ステップS206では、ステップS204で算出されたハッシュ値とステップS205で算出されたハッシュ値を比較し、一致していれば画像データは本実施例のデジタルカメラ1により撮影された後に改竄されていないものであると判定し、一致しなければ画像データは撮影時から改竄された可能性があるとして判定する。また、ステップS205で、暗号化データが公開鍵で復号化できない場合にも、その画像データは本発明実施例のデジタルカメラ1で撮影されたものではないか、撮影後に変更されたものとみなされる。

【0040】

したがって、本発明実施例の画像改竄検出システムを使用する場合、写真の提出者は、デジタルカメラ1から出力して変更を加えていない画像データを含むファイル（本実施例ではJPEGファイル30）をフロッピー等の記録媒体に記録したもの、あるいは着脱可能な記録媒体であるフラッシュメモリ16をデジタルカメラ1から取り外したものを、印刷した写真と共に、あるいは相手の求めに応じて提出する。受け取り側は、パーソナルコンピュータ20にインストールされ

た検出プログラムを用いて受け取ったファイルを読み込んで調べることにより、そのファイルの画像データがデジタルカメラ 1 から出力された時点から変更されていないということを確認することができる。

【0041】

また、検出プログラムに J P E G ファイル 3 0 等の画像データの画像を表示する機能をもたせることにより、印刷された写真と表示された画像が同一であることを確認することができる。

【0042】

また、本実施例では、J P E G ファイル 3 0 のヘッダ部 3 1 に付加された公開鍵を用いて、暗号を復号化した。検出プログラムが複数の秘密鍵に対応する複数の公開鍵を含むリストを記憶してその中から 1 つの公開鍵を選択して暗号を復号することもできる。これにより、そのため、本発明による特徴データの生成方法、暗号化方法、画像データへの埋め込み方などのアルゴリズムを知る者が、自分で公開鍵と秘密鍵の組み合わせを作成し、本発明と同様の処理をパソコンなどを用いて行い画像データを作成した場合でも、その画像データに付加された公開鍵が、あらかじめ用意された公開鍵のリストに含まれないものであれば、その画像データは改竄された可能性がある判断することができる。なお、画像改竄検出システムに記録される複数の公開鍵が知られたとしても、公開鍵から秘密鍵を算出することはほぼ不可能であるため、秘密鍵が他人に知られる恐れはない。

【0043】

上記の実施例では、J P E G 圧縮したものを画像データとして画像記録媒体に記録したが、本発明は他の圧縮方法で圧縮したものや、無圧縮のデータを画像データとして記録したものにも適用できる。また、本実施例では、特徴データを暗号化して J P E G ファイルの画像データ部分の中に埋め込んで記録したが、本発明としてはヘッダ部に書き込むなど、特徴データは画像データのどの位置にあってもよい。

【図面の簡単な説明】

【図 1】

本発明の実施例におけるデジタルカメラにより画像を記録する手順を示すフロ



ーチャートである。

【図 2】

本発明の実施例によるデジタルカメラを示すブロック図である。

【図 3】

本発明の実施例による画像データの特徴データを算出する方法を説明するための模式図である。

【図 4】

本発明の実施例による J P E G ファイルの構造を説明するための模式図である。

【図 5】

本発明の実施例により画像データの改竄を検出する手順を示すフローチャートである。

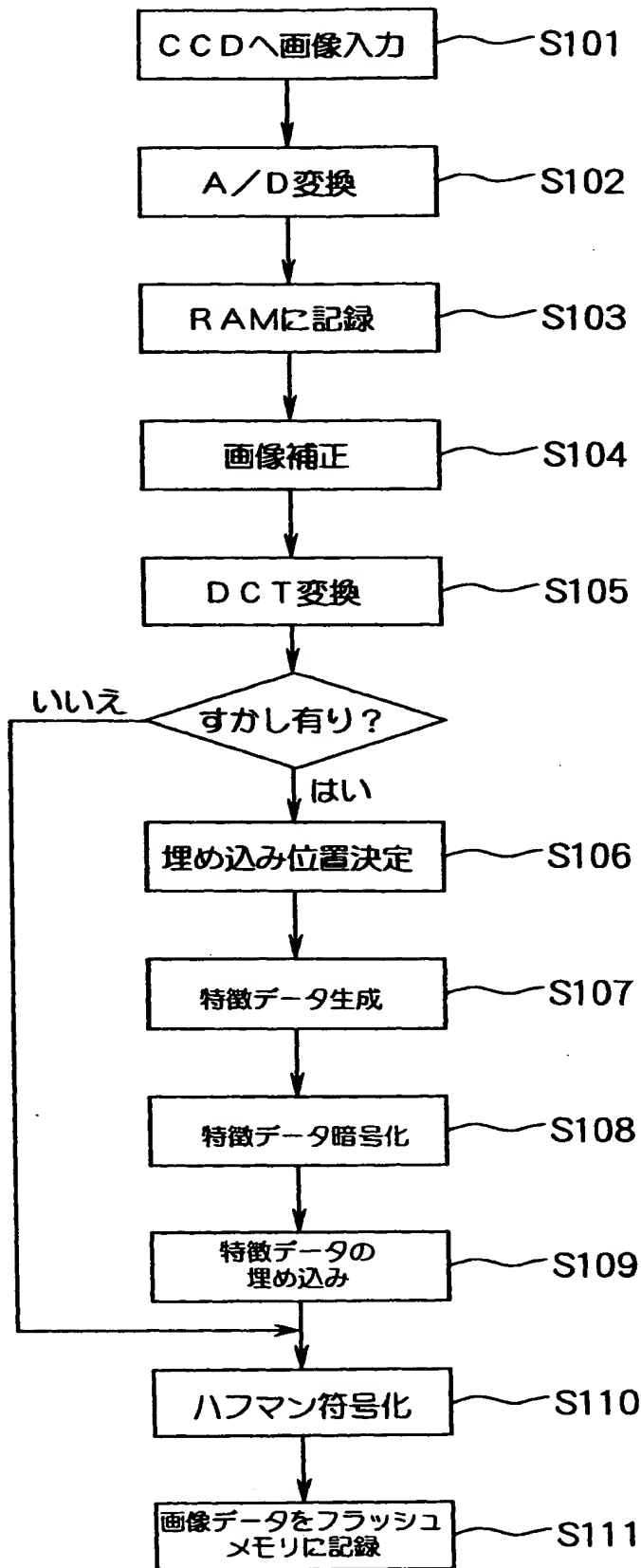
【符号の説明】

- 1 デジタルカメラ
  - 1 1 制御部
  - 1 2 集光レンズ
  - 1 3 C C D (撮像部)
  - 1 4 A / D 変換部
  - 1 5 R A M
  - 1 6 フラッシュメモリ
  - 1 7 インターフェイス
  - 1 8 接続ケーブル
  - 1 9 液晶表示部 ( L C D )
- 2 0 パーソナルコンピュータ
  - 2 1 外部記録媒体
- 3 0 J P E G ファイル
  - 3 1 ヘッダ部
  - 3 2 画像データ
  - 3 3 公開鍵

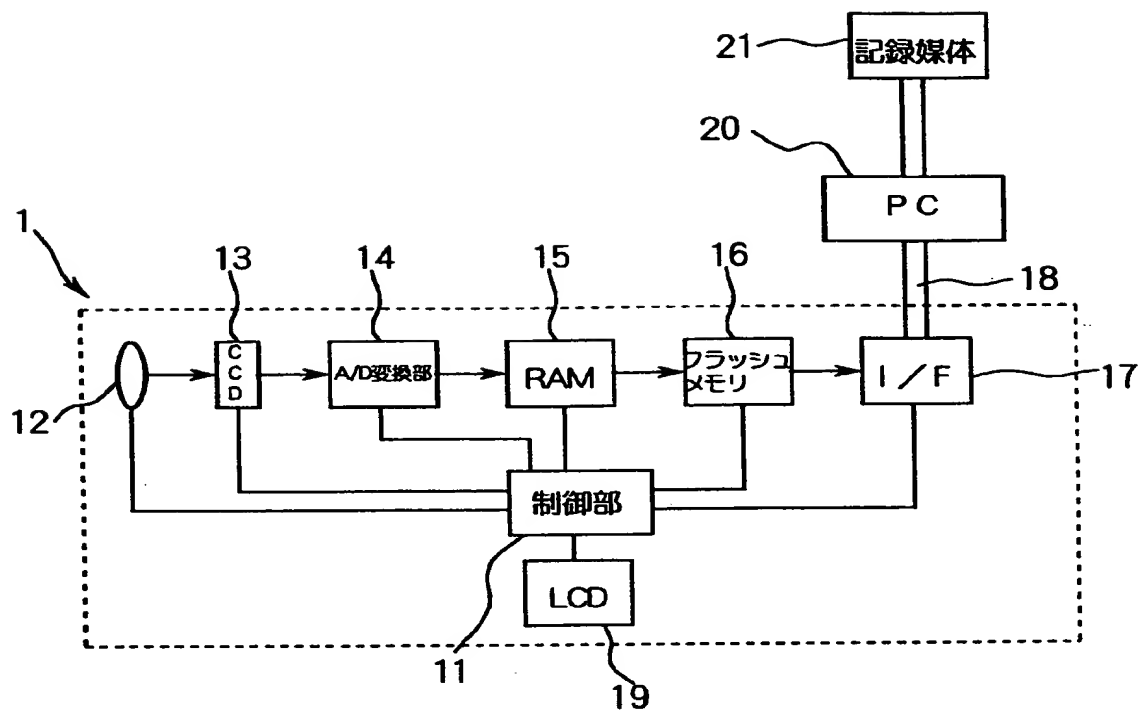
特平 1 1 - 2 5 1 6 6 0

【書類名】 図面

【図 1】



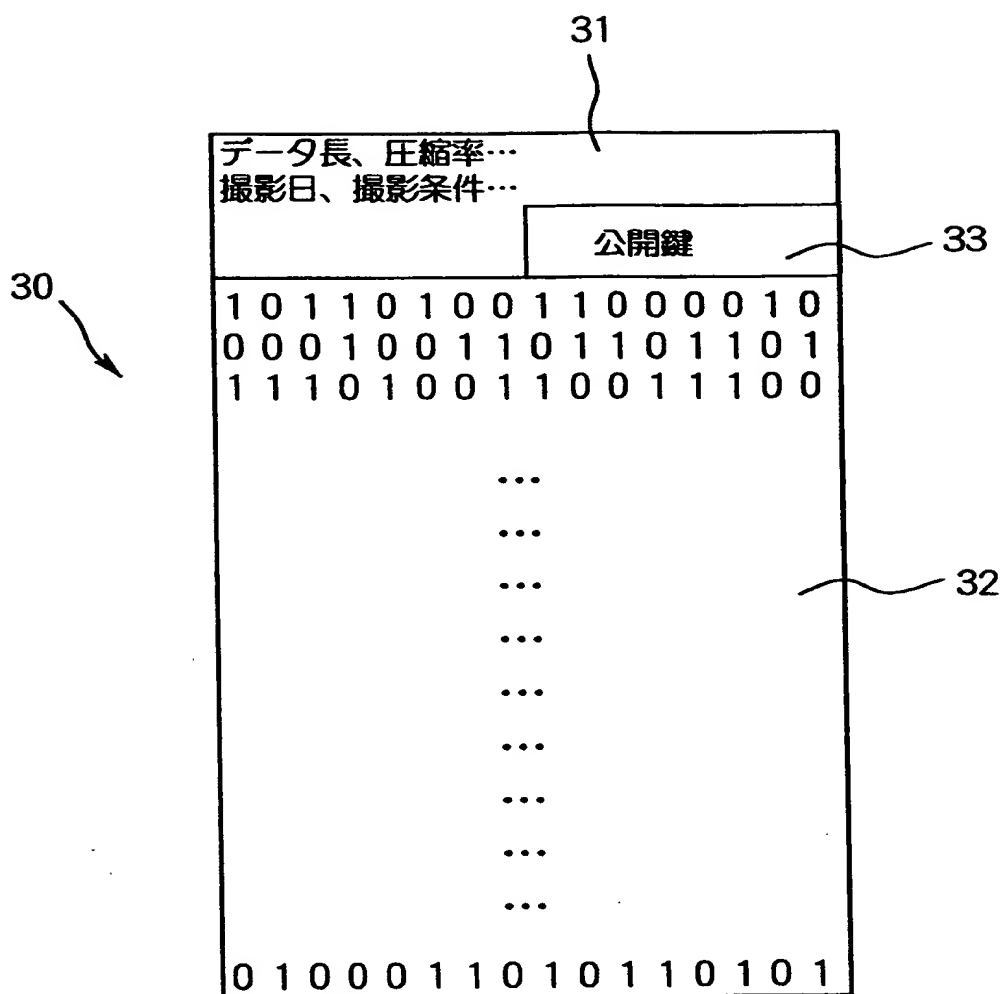
【図 2】



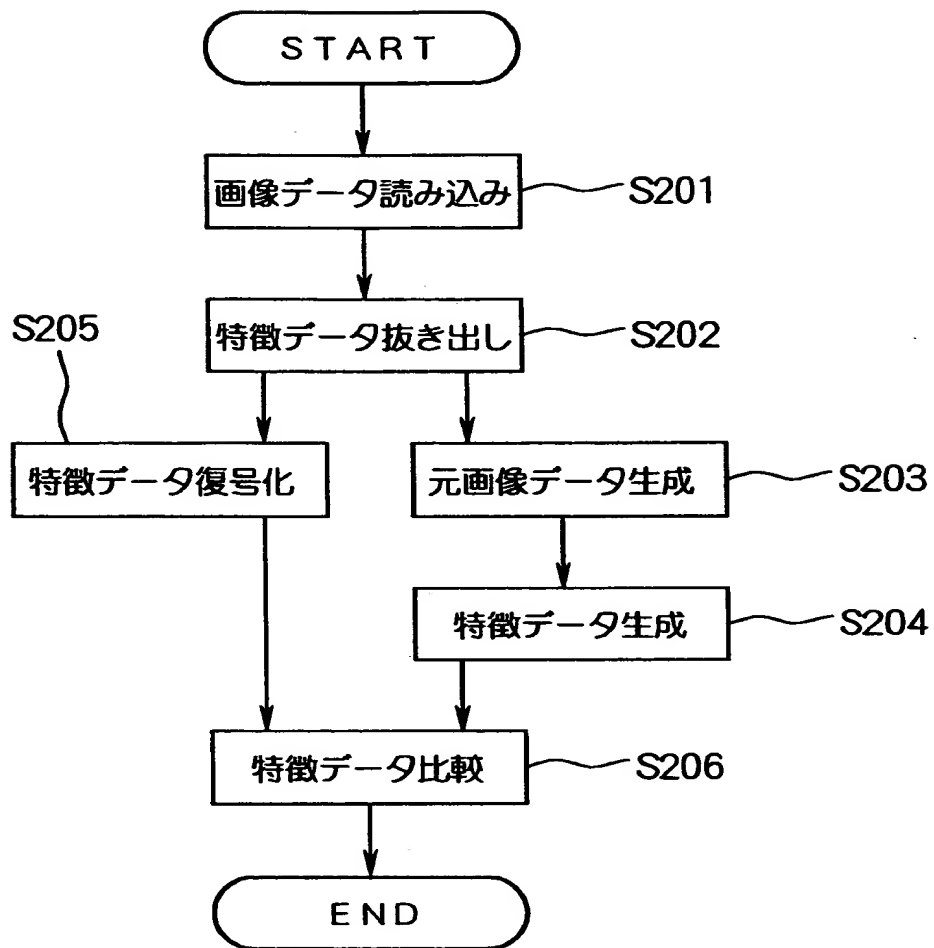
【図 3】

B1	B2	B3 ①	B4 ②
.....00	.....01	.....02	.....FF
B5 ③	B6 ④	B7	B8
.....E5	.....14	.....00	.....01

【図 4】



【図 5】



【書類名】 要約書

【要約】

【課題】 撮影時の画像データから改竄されたか否かを確認することのできる画像データを出力するデジタルカメラを提供する。

【解決手段】 ステップ S 1 0 1 では C C D から出力された電気信号をデジタル信号に変換する。ステップ S 1 0 3 では A / D 変換器から出力されたデジタルデータを R A M に記録する。ステップ S 1 0 4 では R A M に記録されたデータについて各種の画像補正を行う。ステップ S 1 0 5 ～ S 1 1 0 ではステップ S 1 0 4 で補正されたデータを J P E G 方式により圧縮する。ステップ S 1 0 6 で特徴データの埋め込み位置を決定し、ステップ S 1 0 7 で画像データから特徴データを生成する。ステップ S 1 0 8 では特徴データを暗号化して暗号化データとする。ステップ S 1 0 9 では画像データの中に暗号化された特徴データを埋め込む。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000002369]

1. 変更年月日 1990年 8月20日  
[変更理由] 新規登録  
住 所 東京都新宿区西新宿2丁目4番1号  
氏 名 セイコーエプソン株式会社